Attorney Docket No. 9407-3 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Jeffrey S. Bardsley et al.
Application No.: 10/624,344
Filed: July 22, 2003
For: SYSTEMS, METHODS AND DATA STRUCTURES FOR GENERATING COMPUTER-ACTIONABLE COMPUTER SECURITY THREAT MANAGEMENT INFORMATION

Confirmation No.: 7591
Group Art Unit: 2132
Examiner: F. Homayounmehr

October 15, 2007

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

Sir:

This *Appeal Brief* is filed pursuant to the concurrently filed *Notice of Appeal to the Board of Patent Appeals and Interferences*. The present Appeal Brief is being filed in response to the non-final *Office Action* ("*Office Action*") mailed July 25, 2007. As noted at page 2 of the *Office Action*, the filing of the present appeal is appropriate as the pending claims were previously under final rejection, and have not been amended since the issuance of the previous final rejection. Appellants respectfully request that the appeal brief fee from Appellants prior appeal be applied to the present appeal. Appellants are submitting herewith authorization to charge Appellants' deposit account for the difference between the appeal brief fee that was previously paid and the current appeal brief fee. ($510 (current fee) - $500 (previous fee) = $10.00).

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. § 1.136(a). Any additional fees believed to be due may be charged to Deposit Account No. 09-0457.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation of Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that they believe would be affected by the present appeal. Appellants note, however, that Application Serial No. 10/624,158, which is identified as being "related to" the present application, but which is **not** related to the present application by a claim of priority, is currently the subject of an appeal to the Board of Patent Appeals and Interferences. The appeal in Application Serial No. 10/624,158 was filed on July 16, 2007.

Status of Claims

Claims 1-23 remain pending, each of which is finally rejected. Appellants appeal the final rejection of Claims 1-23. The attached Claims Appendix presents the pending claims as rejected in the non-final *Office Action* mailed July 25, 2006.

Status of Amendments

The attached Claims Appendix presents the claims as they currently stand. An *Amendment* was filed in this case on October 11, 2006 in which independent Claims 1, 9 and 18 were amended. This October 11, 2006 *Amendment* was entered. A *Notice of Appeal* was filed on February 2, 2007. In response to Appellants' *Appeal Brief* of April 11, 2007, a non-final *Office Action* was issued on July 25, 2007. Thus, only a single amendment has been filed in this case, and that amendment was entered.

Summary of Claimed Subject Matter

I. Claim 1

Independent Claim 1 is directed to a method of generating computer security threat management information. As shown in **Fig. 3** of the present application, the method of Claim 1 includes three operations, **310**, **320** and **330** which are generally described at page 9, line 25 through page 10, line 3 of the present application. In the first operation **310**, notification of a computer security threat is received. (Specification at page 9, lines 27-28). In operation **320**, a computer-actionable Threat Management Vector (TMV) such as, for example, the TMV **400** illustrated in **Fig. 4** of the present application is generated from the notification that was received in operation **310**. (Specification at page 9, line 29 through page 10, line 1; *see also* Specification at page 10, lines 4-20). This TMV (e.g., TMV **400**) is suitable for use by an automated threat management system such as automated threat management systems that are located at the Target Systems **540** illustrated in **Fig. 5** of the present application. (Specification at page 9, lines 22-24; *see also* Specification at page 11, lines 7-8). In the method of Claim 1, the TMV (e.g., TMV **400**) includes a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (e.g., field **401** in **Fig. 4** of the present application), a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4** of the present application) and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4** of the present application). (Specification at page 10, lines 5-11). As illustrated in operation **330** of **Fig. 3**, the computer-actionable TMV that is generated (e.g., TMV **400** of **Fig. 4**) is transmitted to a plurality of target systems (e.g., target systems **540** of **Fig. 5**) for processing by the plurality of target systems. (Specification at page 10, lines 1-3).

II. Claim 9

Independent Claim 9 is directed to a system for generating computer security threat management information. An example of such a system is the CSIRT server **510** of **Fig. 5** of the present application. The system (e.g., server **510**) includes a Threat Management Vector (TMV) generator, such as message encoder **520** of **Fig. 5**, that is configured to generate a computer-actionable TMV (e.g., TMV **400** of **Fig. 4**) that is suitable for use by an automated threat management system such as, for example, the automated threat management systems that may be located at the Target Systems **540** illustrated in **Fig. 5** of the present application. (Specification at page 10, line 23 through page 11, line 8). The TMV generator (e.g., message encoder **520** of **Fig. 5**) generates the TMV (e.g., TMV **400** of **Fig. 4**) from a notification of a computer security threat that is received, for example, from one of the sources **110, 120, 130, 160, 170, 180** or **190** of **Fig. 5**. (Specification at page 10, line 23 through page 11, line 8). The TMV (e.g., TMV **400** of **Fig. 4**) includes a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (e.g., field **401** in **Fig. 4**), a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4**) and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4**). (Specification at page 10, lines 5-11).

III. Claim 18

Independent Claim 18 is directed to a computer-actionable computer security Threat Management Vector (TMV) such as the TMV **400** of **Fig. 4**. (Specification at page 10, lines 4-20). The TMV includes (1) a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat (e.g., field **401** in **Fig. 4**), (2) a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4**) and (3) a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4**). (Specification at page 10, lines 5-11). The TMV is in a format suitable for use by an automated threat management system such as, for example, the automated threat management systems that may be located at the Target Systems **540** illustrated in **Fig. 5**. (Specification at page 9, lines 22-24; *see also* Specification at page 11, lines 7-8).

Grounds of Rejection to be Reviewed on Appeal

1. The rejections of Claims 1-23 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Application Publication No. 2003/0084349 to Friedrichs et al. ("Firedrichs") in view of U.S. Patent Application Publication No. 2003/0004689 to Gupta et al. ("Gupta").

Argument

I. The Rejections of Claims 1-23 Under 35 U.S.C. § 103 Should Be Reversed

As noted above, Claims 1-23 stand rejected as under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Application Publication No. 2003/0084349 to Friedrichs et al. ("Firedrichs") in view of U.S. Patent Application Publication No. 2003/0004689 to Gupta et al. ("Gupta"). (*Office*

Action at 4-10, ¶ 7). Appellants respectfully submit that these rejections should be reversed for the reasons presented below.

A. Introduction

Friedrichs, the primary reference relied upon in the rejections, is directed to an "early warning system for network attacks." (Friedrichs at Title). In the system/methods of Friedrichs, a plurality of security devices record information relating to security events that occur across a network. (*See, e.g.,* Friedrichs at ¶ 17). Some of this information is then extracted and written into a file having a common format. (*See, e.g.,* Friedrichs at ¶ 18). The information may then be transferred to a database server, where it may be converted into a common, vendor-independent format and analyzed. (*See, e.g.,* Friedrichs at ¶¶ 19 and 23-24). Finally, reports may be generated based on the analyzed data, and these reports are made available to users. (*See, e.g.,* Friedrichs at ¶ 25). The information provided to the user "may contain reports, graphs of security event data and other information related to the processing and analysis of security events and the detection of security incidents", user-requested "specific reports . . . on event data" and/or a "set of reports outlining recent abnormal activity." (Friedrichs at ¶ 26). The reports may be made available to users via a web server, e-mail, pager, facsimile or other delivery mechanisms. (*See, e.g.,* Friedrichs at ¶ 25).

Appellants respectfully submit that Friedrichs is simply another example of the labor-intensive prior art security threat management systems described in the background section of the present application. User's of the system –i.e., individuals – of Friedrichs are provided written reports containing processed security event data. Each such user must then determine how to respond to the security threats contained within the reports and implement such responses. This is exactly the labor-intensive intervention process that embodiments of the present invention avoid.

Gupta does not overcome the deficiencies of Friedrichs. In fact, as discussed in more detail below, Gupta likewise includes no teaching or disclosure of the transmission of computer-actionable TMVs to anything, let alone to a plurality of target systems. Accordingly, for the reasons discussed herein, Appellants respectfully submit that all of the pending claims are patentable over the combination of Friedrichs and Gupta, and hence the rejections of Claims 1-23 under Section 103 should be reversed.

B. The Rejections of Claims 1, 7-10 and 16-17

1. Claim 1

Claim 1 recites:

> 1. A method of generating computer security threat management information, comprising:
>
> receiving notification of a computer security threat;
>
> generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and
>
> transmitting the computer-actionable_TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

Appellants submit that the combination of Friedrichs and Gupta fails to disclose at least three (3) of the recitations of Claim 1. As such, Appellants respectfully submit that the rejection of Claim 1 should be reversed.

a. Friedrichs Does Not Disclose a TMV Having a Field Identifying at Least One System that is Affected by the Security Threat

Appellants first submit that the cited portions of Friedrichs do not disclose a TMV having a field that provides "identification of at least one **system type that is affected by** the computer security threat." In particular, the *Office Action* cites to paragraphs 42 and 35 of Friedrich as disclosing this recitation of Claim 1. (*Office Action* at 5). However, what the cited portion of Friedrichs discloses is a Sensors database **405** that contains demographic information about the location, type and/or operating system of **the security devices that uploaded information** into the All-Events database **or reported the security event**. (Friedrichs at ¶ [0042]). Thus, the information relied on in the rejections relates to the security devices that **report** the security event, and clearly is not information identifying the "system type that is **affected by the computer security threat**" as recited in Claim 1. Appellants respectfully submit that the fact that a security device **reports** a security event does not mean that the reporting security device is **affected by** the computer security threat. In fact, as shown by Gupta (i.e., the secondary reference relied upon in the rejection of Claim 1), specialized devices and systems such as the sensor security modules **27** of Gupta are routinely used to identify security threats to **other** types of devices. Thus, the rejection of Claim 1 should be reversed as Friedrichs simply does not disclose a TMV having a first field that provides "identification of at least one **system type that is affected by** the computer security threat."

b. Friedrichs Does Not Disclose a TMV Having a Field Identifying a Release Level for the System Type Affected

Appellants further submit that the cited portions of Friedrichs do not disclose a TMV having a field that provides "identification of a **release level** for the system type" **that is affected by** the computer security threat. In particular, the *Office Action* cites to paragraph 42 of Friedrich as disclosing this recitation of Claim 1 (*Office Action* at p. 9). However, the "type" information discussed in Friedrichs relates to the type of security device **that is uploading information** as opposed to the type of device that is **affected by** the security threat. In fact, the *Office Action* implicitly concedes as much by stating that Friedrichs "shows detailed specifications of systems **involved** in the security threat", where what Claim 1 recites is that the second field identifies the system type of the system that is **affected by** the threat. (*Office Action* at 9, emphasis added). Moreover, Friedrichs provides no indication that any "release" information is even provided, which is expressly required by the plain language of Claim 1. Thus, the rejection of Claim 1 should also be reversed for each of these additional reasons.

c. Gupta Does Not Disclose Generating a Computer Actionable TMV that is Transmitted to a Plurality of Target Systems

Claim 1 further recites "generating a **computer-actionable** Threat Management Vector (TMV)" that is transmitted "to a plurality of target systems." The *Office Action* concedes that

Friedrichs does not disclose this recitation of Claim 1. (*Office Action* at 5-6). However, the *Office Action* takes the position that "Gupta teaches the creation of a data structure, such as a file, that can be downloaded to the systems to be protected (target systems), such that the target system would mitigate the attacks based on the downloaded file." (*Office Action* at 6). Appellants respectfully submit that this statement overstates the teachings of Gupta, and that Gupta, like Friedrichs, also fails to disclose transmitting a computer-actionable TMV to a plurality of target systems as is recited in Claim 1.

In particular, the cited portion of Gupta discusses downloading an "attack file 149" to a sensor management system 26. However, as made clear by Gupta, the sensor management system 26 is not the "target system." (Gupta at ¶ 0164, stating "A sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform"). Instead, as shown in Fig. 1 of Gupta, the sensor management system 26 is part of a sensor module 27 that is interposed between the target system (i.e., protected server 32) and the enterprise network 30.

More importantly, there is no indication in Gupta that the attack file 149 that is sent to the sensor modules 27 is a "**computer-actionable**" file as recited in Claim 1. Instead, the discussion of the attack file 149 in Gupta just states that the file contains certain types of information. (*See* Gupta at ¶ 0151). Moreover, the discussion of Gupta suggests that the file is **not** computer actionable. For instance, at ¶ 0151, Gupta states that the attack file 149 preferably "suggests responses for such attacks." Such "suggestions" would clearly not be computer actionable information, but instead would be text providing suggestions for an operator or administrator to consider. Likewise, Gupta expressly states that two of the ways that the attack file 149 may be delivered are by e-mail alerts and SMS alert notifications. (Gupta at ¶ 0152). These methods of delivery would generally not result in automatic processing of the attack file, further making clear that the attack file 149 is in the form of, for example, a report, which is no different than the type of information that is provided to the target systems of Friedrichs, and which certainly is not the "computer actionable" file recited in Claim 1.

Thus, for each of the above reasons, Appellants respectfully submit that the rejection of Claim 1 should be reversed.

2. Claims 7-10 and 16-17

Claims 7 and 8 depend from Claim 1, and hence the rejections of Claims 7 and 8 should be reversed for at least each of the reasons that the rejection of Claim 1 should be reversed. Moreover, Claims 9-10, 16 and 17 appear to stand rejected based on the same rationale as Claims 1, 7 and 8, respectively. Accordingly, Appellants respectfully submit that the rejections of Claims 9-10, 16 and 17 should be reversed for at least the same reasons that the rejection of Claim 1 should be reversed.

C. The Rejection of Claim 2

Claim 2 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over the cited art. Claim 2 recites that the "generating" operation of Claim 1 involves "selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format." The *Office Action* cites to paragraphs 40-46 of Friedrichs as disclosing the recitations of Claim 2. However, the cited portion of Friedrichs fails to disclose the recitations of Claim 2 for at least (2) two reasons. First, the cited portions of Friedrichs make no mention of selecting system type, release and possible countermeasures from a database and then converting this information into a computer-readable format for inclusion in a TMV. Second, as conceded in the *Office Action*, the cited portions of Friedrichs are discussing information stored in a database, as opposed to generation of a a TMV that is transmitted to a plurality of target systems as recited in Claim 2. Accordingly, the rejection of Claim 2 should be reversed for these additional reasons.

D. The Rejection of Claim 3

Claim 3 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over the cited art. Claim 3 recites that the "system type comprises a computer operating system type" and that "the release level comprises a computer operating system release level." The *Office Action* cites to paragraphs 35 and 42 of Friedrichs as disclosing the recitations of Claim 3. (*Office Action* at 7). However, the cited portions of

Friedrichs make no mention of the "release level" as recited in Claim 3. Accordingly, the rejection of Claim 3 should be reversed for these additional reasons.

E. The Rejection of Claim 4

Claim 4 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over the cited art. Claim 4 recites that "the set of possible countermeasures comprises an identification of a countermeasure mode of installation." The *Office Action* cites to paragraph 45 of Friedrichs as disclosing the recitations of Claim 4. (*Office Action* at 7-8). However, paragraph 45 of Friedrichs discusses a separate Vulnerabilities database 440 and a Product database 450. The product database may include details on how to patch a particular flaw. However, there is no indication that the information in the Products database **is in a computer-actionable format**, and it is clear that the information in the Products database 450 is not part of the report (i.e., the alleged TMV) that is sent to the users. Accordingly, the rejection of Claim 4 should be reversed for these additional reasons.

The *Office Action* also takes "official notice" that an installation mode for a patch would have been obvious to one skilled in the art. (*Office Action* at 8). However, what Claim 4 recites is that the third field of the TMV that includes the countermeasures includes identification of a mode of installation. Appellants respectfully submit that there has not been, nor can there be, a showing that it would have been obvious to include the mode of installation information in a specific field of a computer actionable TMV as recited in Claim 4. Thus, the resort to official notice also fails to overcome Appellants' showing that Claim 4 is independently patentable over the cited art.

F. The Rejection of Claim 5

Claim 5 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over the cited art. Claim 5 recites that "at least one of the identifications comprises a pointer." The *Office Action* takes "official notice" that "pointers are broadly used in databases to identify data," implicitly conceding that the recitation of Claim 5 is not disclosed in the cited art. (*Office Action* at 8). However, even, assuming, for the sake of argument, that pointers are broadly used in databases, what Claim 5 recites is that at least one of the identifications contained in a third field of a computer actionable TMV that is transmitted to a plurality of target systems comprises a pointer. The *Office Action* has not, and Appellants respectfully submit cannot, take official notice that the combination of Friedrichs and Gupta would include such a pointer. Accordingly, the rejection of Claim 5 should be reversed for these additional reasons.

G. The Rejection of Claim 6

Claim 6 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over the cited art. Claim 6 recites that the TMV further includes "a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level." The *Office Action* states that the description of the Security Device 110 and Hunter server 140 in paragraph [0022] of Friedrich discloses the recitations of Claim 6. (*Office Action* at 7 and 10-11). Notably, the *Office Action* does not even attempt to explain how these devices of Friedrichs correspond to the recitations of Claim 6, and Appellants respectfully submit that no such explanation could be provided. Accordingly, the *Office Action* likewise has failed to make a *prima facie* rejection with respect to the recitations added by Claim 6, and the rejection of Claim 6 should be reversed for this additional reason.

H. The Rejection of Claim 11

Claim 11 depends from Claim 9 and hence is patentable for at least the reasons, discussed above, that Claim 9 is patentable over the cited art. Claim 11 recites that the system includes a "common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format, wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat." The *Office Action* takes the position that Fig. 4 of Friedrichs and associated text discloses "a common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format." (*Office Action* at 9). Appellants respectfully submit, however, that this is not the case. More importantly, Friedrichs clearly does not disclose making a TMV generator . . . responsive to the common semantics database" as recited in Claim 11. Furthermore, while the *Office Action* takes the position that generating reports based on user defined parameters was a well known feature of databases, that certainly is not a showing that generation of computer actionable TMVs was a well known function of databases, which is what is recited in Claim 11. Accordingly, the rejection of Claim 11 should be reversed for these additional reasons.

I. The Rejection of Claim 11

Claim 11 appears to stand rejected based on the same rationale as Claim 2. Accordingly, Appellants respectfully submit that the rejection of Claim 11 should be reversed for the same reasons, discussed above, that the rejections of Claim 2 should be reversed.

J. The Rejection of Claim 12

Claim 12 appears to stand rejected based on the same rationale as Claim 3. Accordingly, Appellants respectfully submit that the rejection of Claim 12 should be reversed for the same reasons, discussed above, that the rejections of Claim 3 should be reversed.

K. The Rejection of Claim 13

Claim 13 appears to stand rejected based on the same rationale as Claim 4. Accordingly, Appellants respectfully submit that the rejection of Claim 13 should be reversed for the same reasons, discussed above, that the rejections of Claim 4 should be reversed.

L. The Rejection of Claim 14

Claim 14 appears to stand rejected based on the same rationale as Claim 5. Accordingly, Appellants respectfully submit that the rejection of Claim 14 should be reversed for the same reasons, discussed above, that the rejections of Claim 5 should be reversed.

M. The Rejection of Claim 15

Claim 15 appears to stand rejected based on the same rationale as Claim 6. Accordingly, Appellants respectfully submit that the rejection of Claim 15 should be reversed for the same reasons, discussed above, that the rejections of Claim 6 should be reversed.

N. The Rejections of Claims 18 and 23

Claims 18 and 23 appear to stand rejected based on the same rationale as Claims 1 and 8, respectively. Accordingly, Appellants respectfully submit that the rejection of Claims 18 and 23 should be reversed for the same reasons, discussed above, that the rejections of Claims 1 and 8, respectively, should be reversed.

O. The Rejection of Claim 19

Claim 19 appears to stand rejected based on the same rationale as Claim 3. Accordingly, Appellants respectfully submit that the rejection of Claim 19 should be reversed for the same reasons, discussed above, that the rejections of Claim 3 should be reversed.

P. The Rejection of Claim 20

Claim 20 appears to stand rejected based on the same rationale as Claim 4. Accordingly, Appellants respectfully submit that the rejection of Claim 20 should be reversed for the same reasons, discussed above, that the rejections of Claim 4 should be reversed.

Q. The Rejection of Claim 21

Claim 21 appears to stand rejected based on the same rationale as Claim 5. Accordingly, Appellants respectfully submit that the rejection of Claim 21 should be reversed for the same reasons, discussed above, that the rejections of Claim 5 should be reversed.

R. The Rejection of Claim 22

Claim 22 appears to stand rejected based on the same rationale as Claim 6. Accordingly, Appellants respectfully submit that the rejection of Claim 22 should be reversed for the same reasons, discussed above, that the rejections of Claim 6 should be reversed.

II. Conclusion

In light of the above, Appellants submit that each of the pending claims is patentable over the cited references and, therefore, request reversal of the rejections of Claims 1-23 under 35 U.S.C. § 103.

Respectfully submitted,

D. Randal Ayers

D. Randal Ayers
Registration No. 40,493

USPTO Customer No. 20792
Myers Bigel Sibley & Sajovec, P.A.
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

CERTIFICATION OF ELECTRONIC TRANSMISSION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office on October 15, 2007.

Michele P. McMahan

Michele P. McMahan
Date of Signature: October 15, 2007

CLAIMS APPENDIX

Pending Claims USSN 10/624,344
Filed July 22, 2003

1. A method of generating computer security threat management information, comprising:

receiving notification of a computer security threat;

generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and

transmitting the computer-actionable TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

2. A method according to Claim 1 wherein the generating comprises selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format.

3. A method according to Claim 1 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

4. A method according to Claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

5. A method according to Claim 1 wherein at least one of the identifications comprises a pointer.

6. A method according to Claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

7. A method according to Claim 6 wherein the subsystem type comprises an application program type.

8. A method according to Claim 1 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

9. A system for generating computer security threat management information, comprising:

a Threat Management Vector (TMV) generator that is configured to generate a computer-actionable TMV that is suitable for use by an automated threat management system from a notification of a computer security threat that is received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level.

10. A system according to Claim 9 wherein the TMV generator is also configured to transmit the TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

11. A system according to Claim 9 further comprising a common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format, wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat.

12. A system according to Claim 9 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

13. A system according to Claim 9 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

14. A system according to Claim 13 wherein the set of possible countermeasures further comprises a pointer to a remediation to be applied as a countermeasure.

15. A system according to Claim 9 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

16. A system according to Claim 15 wherein the subsystem type comprises an application program type.

17. A system according to Claim 9 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

18. A computer-actionable computer security Threat Management Vector (TMV) comprising:

a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat;

a second computer-readable field that provides identification of a release level for the system type; and

a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level,

wherein the TMV is in a format suitable for use by an automated threat management system.

19. A TMV according to Claim 18 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

20. A TMV according to Claim 18 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

21. A TMV according to Claim 18 wherein at least one of the identifications comprises a pointer.

22. A TMV according to Claim 18 further comprising:

a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat;

a fifth computer-readable field that provides identification of a release level for the subsystem types; and

wherein the third computer-readable field provides identification of a set of possible countermeasures for a subsystem type and a release level.

23. A TMV according to Claim 18 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

EVIDENCE APPENDIX

No evidence is being submitted with this *Appeal Brief* pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.